IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA v. PAUL CHRETIEN	Criminal No. 19-262

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (DOC. NO. 29)

AND NOW comes the United States of America, by its attorneys, Scott W. Brady, United States Attorney for the Western District of Pennsylvania, and Heidi M. Grogan, Assistant United States Attorney for said District, and respectfully submits the government's Response to defendant Paul Chretien's Suppression Motion:

I. INTRODUCTION

On August 27, 2019, a federal grand jury charged defendant Paul Chretien in a seven-count Indictment in violation of: Title 18, United States Code §§ 2252(a)(2) and 2252(b)(1)—Distribution of Material Depicting the Sexual Exploitation of a Minor (Counts One through Three and Counts Five and Six); Title 18, United States Code §§ 2252(a)(2) and 2252(b)(1)—Receipt of Material Depicting the Sexual Exploitation of a Minor (Count Four); and Title 18, United States Code, § 2252(a)(4)(B) and 2252(b)(2)—Possession of Material Depicting the Sexual Exploitation of a Minor (Count Seven). All counts stem from alleged criminal conduct occurring on distinct dates between August 2018 through November 2018, during which time defendant Paul Chretien was communicating with an individual via Google Hangouts and distributed and/or received digital images of a minor engaging in sexually explicit conduct or child pornography. The government further alleges that defendant possessed visual depictions of minors engaged in sexually explicit conduct (child pornography) on or about February 6, 2019.

On December 25, 2019, defendant, through counsel, filed his motion to suppress evidence. Doc. No. 29. The government now submits the following in support of its opposition to defendant's motion. For the reasons set forth below, the government respectfully urges the Court to deny defendant's motion.

II. MOTION TO SUPPRESS EVIDENCE

On February 5, 2019, Detective Steven Dish of the Allegheny County Police Department applied for a warrant to search the location in Bridgeville, Pennsylvania that law enforcement had identified as the place where defendant Paul Chretien resided. Defendant now moves to suppress evidence recovered from this location, as well as any evidence resulting from subsequent search warrants and any subsequent incriminating statements made by defendant. The Court should deny defendant's motion because law enforcement searched defendant Chretien's residence only after obtaining a valid search warrant supported by probable cause.

A. Defendant Has No Right to an Evidentiary Hearing

As the Third Circuit has recognized, while defendants may file motions to suppress evidence prior to trial, "evidentiary hearings on such matters are not granted as a matter of course." *United States v. Hines*, 628 F.3d 101, 105 (3d Cir. 2010). To require a hearing on a motion to suppress, the motion must raise "issues of fact material to the resolution of the defendant's constitutional claim." *United States v. Voigt*, 89 F.3d 1060, 1067 (3d Cir 1996). In other words, the defendant must raise a "colorable claim" that his constitutional rights were violated. To raise such a claim, a defendant must do more than make "bald-faced allegations of misconduct." *Id.* Instead, "a motion to suppress must be detailed enough to present both a colorable constitutional claim and disputed issues of material fact that will affect a district court's resolution of the motion." *United States v. Blackman*, 407 F. App'x 591, 594-95 (3d Cir. 2011) (citing *Voigt*, 89 F.3d at

1067). An evidentiary hearing is only required if a defendant's motion alleges facts that are "sufficiently specific, non-conjectural, and detailed to enable the court to conclude" that a substantial claim is presented. *Hines*, 628 F.3d at 105; *see also United States v. Durante*, 612 F. App'x 129, 131 (3d Cir. 2015) (affirming district court's refusal to hold an evidentiary hearing on a motion to suppress the fruits of a consent search, where defendant "offered no clear basis for his assertion" that his wife's consent was not voluntary).

The burden of proof is on the defendant, and is not shifted to the government unless and until the defendant establishes a colorable basis for the claim. *United States v. Johnson*, 63 F.3d 242, 245 (3d Cir. 1995); *United States v. Benoit*, 730 F.3d 280, 288 (3d Cir. 2013) ("Only 'once the defendant has established a basis for his motion' does the burden shift to the government to show the search was reasonable.") (citing *Johnson*). It is not enough for the defendant to simply state that his arrest was illegal or lacked probable cause. *Voigt*, 89 F.3d at 1067; *see also United States v. Jackson*, 363 F. App'x 208, 210 (3d Cir. 2010) (upholding district court's refusal to hold an evidentiary hearing on a motion to suppress a warrantless search, where the defendant failed to offer any version of events contrary to events detailed in the police report). Rather, a defendant must put forth some facts which enable the court to determine that a substantial claim is present. *See United States v. Persinger*, 284 Fed. App'x 885, 887 (3d Cir. 2008) ("A district court is not always obligated to conduct an evidentiary hearing in conjunction with a motion to suppress, but need only do so 'if the difference in facts is material, that is, only if the disputed fact makes a difference in the outcome.") (quoting *United States v. Juarez*, 454 F.3d 717, 720 (7th Cir. 2006)) (internal quotation and citation omitted).

As the Third Circuit recognizes, "the purpose of an evidentiary hearing in the context of a suppression motion is to assist the court in ruling upon a defendant's specific allegations of

unconstitutional conduct—its purpose is not to assist the moving party in making discoveries that, once learned, might justify the motion after the fact." *Hines*, 628 at 105. As such, the Court requires defendants to "(1) state a colorable legal claim, (2) identify facts material to that claim, (3) show why the facts are disputed, and then (4) request a hearing to resolve the dispute." *Id.* at 108.

Here, defendant has not advanced any fact in dispute necessitating a hearing. Thus, the Court should deny defendant's request without a hearing.

B. Legal Standard—Review of Search Warrants

A search with a search warrant is presumed lawful, and the preliminary burden is on the defendant to invalidate it by defeating its presumption of regularity. *Franks v. Delaware*, 438 U.S. 154, 156 (1978). "All data necessary to show probable cause for the issuance of a search warrant must be contained within the four corners of a written affidavit given under oath." *People of the Virgin Islands v. John*, 654 F.3d 412, 420 (3d Cir. 2011) (citing *United States v. Gourde*, 440 F.2d, 1065, 1067 (9th Cir. 2006)).

The task of a federal district court judge reviewing whether a search warrant was supported by probable cause is to determine whether the judge who issued the search warrant had a substantial basis for concluding that there was a fair probability that contraband or evidence of present or past criminal activity will be found at a particular place. *United States v. Stearn*, 597 F.3d 540, 554 (3d Cir. 2010); *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002) (citing *United States v. Harvey*, 2 F.3d 1318, 1322 (3d Cir. 1993) and *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Probable cause exists when there is "a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Bond*, 581 F.3d 128, 139 (3d Cir. 2009) (quoting *United States v. Burton*, 288 F.3d 91, 103 (3d Cir. 2002); and *Gates*, 462

U.S. at 238. In *Gates*, the Supreme Court explained that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of rules." *Id.* at 232. The Court continued, "[fi]nely-tuned standards such as proof beyond a reasonable doubt or by the preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision . . . it is clear that only the probability, and not a prima facie showing, of criminal activity is the standard for probable cause." *Id.* at 235. Probable cause "is not a high bar"; it "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). Probable cause is a "commonsense, nontechnical conception[] that deal[s] with the factual and practical considerations of everyday life on which reasonable and prudent [people], not legal technicians, act." *United States v. Laville*, 480 F.3d 187, 196 (3d Cir. 2007) (citing *Ornelas v. United States*, 517 U.S. 690, 695 (1996)) (internal quotations marks omitted).

In reviewing a claim that probable cause of criminal activity was lacking, a reviewing court must keep in mind that there is a fundamental difference between the level of proof required to support a conclusion of guilt and the level of proof required to support a conclusion of probable cause. *Laville*, 480 F.3d at 194. In fact, to find probable cause a reviewing court "need not conclude that it was 'more likely than not' that the evidence sought was at the place described." *Bond*, 581 F.3d at 139 (emphasis added). "Direct evidence linking the place to be searched to the crime is not required for the issuance of a search warrant." *Id.* (citing *Hodge*, 246 F.3d 301, 305 (3d Cir. 2001) (internal citations omitted). "This is because probable cause can be, and often is, inferred by considering the type of crime, the nature of the items sought, the suspect's opportunity for concealment and normal inferences about where a criminal might hide the fruits of his crime." *Id.*

The magistrate judge "is entitled to draw reasonable inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense." *Hodge*, 246 F.3d, 305 (3d Cir. 2001). "In assessing whether probable cause exists, statements in an affidavit may not be read in isolation—the affidavit must be read as a whole." *United States v. Conley*, 4 F.3d 1200, 1208 (3d Cir. 1993). Moreover, the "issuing judge or magistrate may give considerable weight to the conclusions of experienced law enforcement officers." *United States v. Whitner*, 219 F.3d 289, 296 (3d Cir. 2000). In reviewing prior probable cause determinations, "the role of the courts is not that of the much-maligned 'Monday morning quarterback' whose critiques are made possible only by the benefits of hindsight." *Dempsey v. Bucknell Univ.*, 834 F.3d 457, 469 (3d Cir. 2016). This is so, at least in part, because the probable cause standard "does not require that officers correctly resolve conflicting evidence or that their determinations of credibility, were, in retrospect, accurate. . . ." *Id*. at 480 (citing *Wright v. City of Philadelphia*, 409 F.3d 595, 603 (3d Cir. 2005)).

A reviewing court must pay great deference to the issuing magistrate's decision. *Harvey*, 2 F.3d at 1322; *Conley*, 4 F.3d at 1205. The reviewing court is not to conduct a *de novo* review of the probable cause determination because "even if [the] reviewing court would not have found probable cause in a particular case, it must nevertheless uphold a warrant so long as the issuing magistrate's determination was made consistent with the minimal substantial basis standard." *Id.* A "'grudging or negative attitude by reviewing courts towards warrants' is inconsistent with the Fourth Amendment's strong preference for searches conducted pursuant to a warrant." *United States v. Jones*, 994 F.2d 1051, 1057 (3d Cir. 1993) (quoting *United States v. Ventresca*, 380 U.S. 102, 109 (1965)). Thus, the United States Supreme Court has noted that the practical nature of evaluating probable cause justifies great deference upon review and calls for

upholding the authorizing judge's findings even in marginal or doubtful cases. *Ventresca*, 380 U.S. at 109; *see also United States v. Nixon*, 918 F.2d 895, 900 (11th Cir. 1990).

C. The Search Warrant Was Supported by Probable Cause

Allegheny County Police Department Detective Steven Dish's affidavit in support of his application for a warrant for defendant Paul Chretien's residence in Bridgeville, Pennsylvania provided ample evidence in support of the issuing Judge's probable cause finding. Defendant's suppression motion attacks the issuing Judge's finding of probable cause alleging that: (1) the information was insufficient to establish a fair probability that contraband or evidence of a crime would be found in the place to be searched; and (2) the information contained within the affidavit was stale. Defendant's motion has no merit and should be denied without a hearing.

1. Detective Dish's affidavit demonstrated probable cause to believe evidence of criminal activity would be found at defendant's residence

Here, the issuing Judge had a substantial basis for determining there was a fair probability that contraband or evidence of a crime would be found in the place to be searched—defendant's residence. The search warrant application and accompanying affidavit was attached as an exhibit to defendant's motion.

Where an affidavit supporting a search warrant "link[s] the IP address in question to both child pornography and to the residential address" searched, and also includes a "discussion of [the] computer technology" supporting that connection, there is a "strong suggestion" that the computer used to access child pornography "would be found at the [address] and would contain evidence associated with child pornography and/or its transmission." *United States v. Renigar*, 613 F.3d 990, 994 (10th Cir. 2011) (citing *United States v. Vosburgh*, 602 F.3d 512 (3d Cir. 2010) ("conclud[ing] that it was fairly probable that instrumentalities or evidence of [child pornography]—such as computers and computer equipment—would be found in [the defendant's]

apartment," *id.* at 527 (internal quotation marks omitted), based upon an affidavit which "explained that . . . someone using a computer with [a certain] IP address . . . attempted to download a video that purported to be hardcore child pornography . . . [and] that on the day in question, the relevant IP address was assigned to a Comcast account registered to [the defendant's] apartment," *id.* at 526.") and *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) ("conclud[ing] that it was 'clear that there was a substantial basis to conclude that evidence of criminal activity would be found at [the defendant's address],' based upon an affidavit which 'included the information that . . . child pornography . . . had been transmitted over [a certain] IP address . . . and that this IP address was assigned to [the defendant]" who resided at the address listed in the affidavit.").

The search warrant affidavit here specified that law enforcement requested permission to search for evidence of violations of the Pennsylvania Statute that criminalizes the sexual abuse of children—Title 18, Pa.C.S.A. Crimes and Offenses § 6312(b), (c), (d). This Pennsylvania law provides in relevant part:

> **(b) Photographing, videotaping, depicting on computer or filming sexual acts.-** (1) Any person who causes or knowingly permits a child under the age of 18 years to engage in a prohibited sexual act or in the simulation of such act commits an offense if such person knows, has reason to know or intends that such act may be photographed, videotaped, depicted on computer or filmed.
> (2) Any person who knowingly photographs, videotapes, depicts on computer or films a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such an act commits an offense.
> **(c) Dissemination of photographs, videotapes, computer depictions and films.-** Any person who knowingly sells, distributes, delivers, disseminates, transfers, displays or exhibits to others, or who possesses for the purpose of sale, distribution, delivery, dissemination, transfer, display or exhibition to others, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act commits an offense.
> **(d) Child pornography.--**Any person who intentionally views or knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act commits an offense.

In his affidavit, Detective Dish provided sufficient facts to support a finding of probable cause that defendant had violated this Pennsylvania law and that defendant still possessed evidence, fruits, and instrumentalities of the violation with him at his residence. This is because Detective Dish established a sufficient nexus between the criminal act and the residence to be searched. Detective Dish explained that Google reported to the National Center for Missing and Exploited Children ("NCMEC") two separate occasions where it discovered of an image of apparent child pornography was uploaded by a user and stored in Google Photos. Google reported each of these occasions as a "cybertip" to NCMEC. Specifically, Detective Dish reported that Google discovered the uploaded image of child pornography on May 1, 2018 at 11:23:53 UTC and on May 4, 2018 at 11:23:59 UTC, respectively. On both occasions when it made the cybertips, Google reported that the image of child pornography was from a person with the name Carol Gretski, with a particular phone number (207-458-5506), and using the email address gretskicarol@gmail.com. Google further reported to NCMEC the unique IP address from which the account was logged onto and registered to Google on a specific date and time—April 30, 2018 at 19:40:50 UTC. ("UTC," or "Universal Time Coordinated" is the time standard commonly used across the world and must be adjusted to reflect Eastern Standard Time).

Detective Dish stated that he viewed the uploaded image as sent by Google via NCMEC and the image depicts a prepubescent female child under the age of 18 years old exposing her genitals in a sexual act and/or pose. Thus, the affidavit established probable cause that the user of the "Carol Gretski" account had violated Pennsylvania law by intentionally viewing and/or knowingly possessing an image of child pornography.

In the affidavit, Detective Dish explained that, based on this information, he then took steps to obtain further information regarding the unique IP address from which "Carol Gretski" was accessing Google. Detective Dish explained that he performed a search to find out which internet service provider or "ISP" serviced the particular IP address associated with the information provided by Google to NCMEC. Within previous paragraphs in the affidavit, Detective Dish had explained how every machine that is on the Internet has a unique Internet Protocol Address or "IP" and that the American Registry for Internet Numbers (ARIN) is the organization that manages Internet numbering resources for North America. Detective Dish further explained that this is important because IP numbers are "globally unique, numeric identifiers that computers use to identify hosts and networks connected to the Internet." The affiant further explained how ARIN works—specifically ARIN's role in allocating and assigning IP blocks to ensure continued operation of the Internet. Detective Dish explained that ARIN maintains a "routing registry where network operators can submit, maintain, and retrieve router configuration information." Because of this, Detective Dish was able to look up the unique IP associated with the Google account that had Google had twice reported to NCMEC because the user had uploaded and stored an apparent image of child pornography. Detective Dish learned that this unique IP belonged to Comcast Cable Communications, LLC ("Comcast").

Detective Dish then used this information to obtain a search warrant for subscriber information from Comcast for the particular IP address as of the date and time that Google reported that the user of the account that had uploaded the apparent images of child pornography had been logged onto Google (April 30, 2019 at 19:40:50 UTC). Detective Dish explained in his affidavit that Comcast responded that defendant Paul Chretien was the subscriber of the unique IP with a service address of 50 Vanadium Road, Apartment 137, Bridgeville, PA 15107. Comcast further

provided a telephone number for the subscriber of the IP as 207-458-5506 and an email address of pvchreitien@comcast.com. This phone number was the same phone number previously provided by Google to NCMEC as being associated with "Carol Gretski."

Detective Dish also explained how he also applied for and received information pursuant to a search warrant for the Google account of "Carol Gretski." In response, Google confirmed that the account was subscribed to by a user in the name of Carol Gretski, created on April 30, 2018, with the unique IP address Google had previously provided to NCMEC. Detective Dish noted that Google again provided the image that was submitted in association with the two previous cybertips – both cybertips images were of the same prepubescent female child exposing her genitals in a sexual act/pose.

Finally, the affiant explained how Detective Dish then confirmed that an individual named Paul Vincent Chretien had a valid Pennsylvania Driver's License at the exact Bridgeville, Pennsylvania address that Comcast had identified as being subscribed to by Paul Chretien and associated with the IP address that had been logged onto the Google account created on April 30, 2018 wherein several days after the account's creation (May 1 and May 4, 2018), Google discovered an uploaded image of child pornography stored in Google Photos.

In addition to detailing his investigative efforts, the affiant also detailed his training and experience in investigating computer crimes and child pornography. At the outset of his affidavit, Detective Dish detailed his 25 years of experience in law enforcement, including his extensive experience in investigating crimes involving the sexual exploitation of children, including via the Internet and in crimes involving the illegal transmission or possession of child pornography. Later within his affidavit, Detective Dish explained his knowledge of computer forensics—how he knows that deleted computer files can be recovered and, similarly, how files viewed via the Internet

are automatically downloaded into a temporary Internet directory or "cache" that often can be retrieved from a computer's hard drive. Detective Dish explained that law enforcement's ability to retrieve such files depends "less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits."

Detective Dish further explained how, in his training and experience in investigating crimes involving child pornography, he knows that "child pornographers generally prefer to store images of child pornography in electronic form" and how a computer's ability to store "tens of thousands of images at high resolution" makes computers "an ideal repository for [child] pornography" and that these images "can be easily sent to or received from other computer users over the Internet." Detective Dish's affidavit also detailed the volume of evidence that he knows computers can hold and explained why he believes that such information would still be found on devices located at defendant Paul Chretien's Bridgeville address. This is because, in his training and experience, Detective Dish has learned that "persons engaged in the distribution and possession of pornographic/child pornographic materials often maintain collections of such material and such material is used as a resource for furtherance of the exploitation of juveniles. The collections are kept by these persons for long periods of time, years at times."

Upon review of the information contained in Detective Dish's affidavit, Judge Cashman of Pennsylvania's Court of Common Pleas issued a warrant for the residential address in Bridgeville, Pennsylvania for evidence of violations of Pennsylvania law as found at 18 P.A.C.S. § 6312(b), (c), (d).

Contrary to defendant's assertion, the affidavit does indicate when the images were uploaded. Google's response to legal process indicated that the account for "Carol Gretski" had been created on April 30, 2018 at 19:40:50 UTC. Within one day of the account being created—

on May 1, 2018, Google discovered an image of child pornography uploaded and stored in Google photos; the image was discovered in Google photos again on May 4, 2018. The reasonable inference from this information included in the affidavit is that the user of the "Carol Gretski" Google account uploaded the image between April 30, 2018 and May 4, 2018. Regardless of when the image was uploaded, the inclusion of these facts in the affidavit established probable cause that the user of the "Carol Gretski" account was intentionally viewing and/or knowingly possessed an image of child pornography—a violation of the Pennsylvania law set forth in the affidavit.

These facts, taken as a whole, demonstrated probable cause to believe that evidence of criminal activity would be found at defendant's residence and this Court should find that the search warrant for defendant's residence was valid.

2. The information in the affidavit was relevant and not stale

Defendant argues that the information in the affidavit was too stale to support a finding of probable cause. Defendant is simply wrong.

Staleness is a matter of whether probable cause exists, at the time of the application for the warrant, to believe that the items to be seized are in the place to be searched. *See United States v. Harvey*, 2 F.3d 1318, 1322 (3d Cir. 1993). Whether information is too stale to establish probable cause depends on "the nature of the crime and the type of evidence" involved. *United States v. Zimmerman*, 277 F.3d 426, 434 (3d Cir. 2002). As the Third Circuit reiterated in the case of *United States v. Vosburgh*, 602 F.3d 512, 528 (3d Cir. 2010), "staleness is not a matter of mechanically counting days." (citing *Zimmerman*, 277 F.3d at 343).

In the context of crimes involving child pornography, the Third Circuit has "long recognized [that] persons with an interest in child pornography tend to hoard their material and retain them for a long time." *Id.* (upholding a four-month gap between target's access of child

pornography link and warrant application and citing two other Third Circuit cases wherein the Court recognized that individuals who possess child pornography rarely dispose of their material). In the case of *United States v. Shields*, the Third Circuit *sua sponte* addressed staleness in the child pornography context where defendant did not raise a staleness challenge. 458 F.3d 269, 279 n.7 (3d Cir. 2006). In the *Shields* case, the Third Circuit stated that had a staleness challenge been raised, it would not have altered the court's decision to uphold a search warrant where nearly nine months had passed between when the child pornography website that the FBI was investigating became defunct and the FBI's search warrant application. *Id.* (explaining that staleness issues are "context dependent" and stating that where information is more "durable" where it suggests a "continuing offense") (internal citations omitted); *see also United States v. Bogle*, Crim. No. 08-335, 2009 WL 1064473 at *3 (W.D. Pa. April 20, 2009) (Diamond, J.) ("The Third Circuit has recognized that individuals rarely, if ever, dispose of child pornography.") (citing cases); *States v. Workman*, Crim. No. 07-00040, 2008 WL 4093717 at *5 (E.D. Pa. Sept. 4, 2008) ("The observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. . . . This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.") (internal quotations omitted).

The principal that collectors of child pornography often store their material and rarely discard it is not negated simply because law enforcement does not have particularized information about the collecting habits of the target. *See Vosburgh*, 602 F.3d at 528 (finding this principal supportive of an affidavit also describing repeated attempts to access a link advertising hard cord child pornography and posted on an underground website dedicated to child pornography and

accessed by an apartment in which the target lived alone). The Court in *Vosburgh* upheld a four-month gap between when defendant accessed a child pornography link and the search warrant application but cautioned that their holding was not "that information concerning child pornography crimes can never grow stale." *Id.* The Court explained that because crimes involving child pornography have a "relatively long shelf life," information about such crimes "has not been, and should not be, quickly deemed stale." *Id.* The Court further expounded that this is because the "type of evidence" involved in child pornography crimes, such as computers and computer equipment, "is not the type of evidence that rapidly dissipates or degrades. Nor is it the type of property that is quickly or continuously discarded." *Id.*

Indeed, courts have recognized the "long shelf life" of child pornography crimes where the crime is alleged to have been committed by use of a computer because a trained forensic examiner has the ability to recover files from a computer, even when they have been deleted by the user. *See, e.g., United States v. Eberle*, Crim. No. 05-26 (Erie), 2006 WL 1705143, at *1 (W.D. Pa. June 15, 2006) (McLaughlin, J.) (upholding a gap of over three and a half year and noting that even when a computer has been 'wiped,' where 'all files and data associated with a prior user from a hard drive [are deleted],' the data may still be retrieved through forensic procedures); *see also United States v. Payne*, 519 F. Supp. 2d 466, 477-78 (D.N.J. 2007) (upholding time frame of less than three months where affidavit detailed "how computers and the internet have 'revolutionized' the methods by which child pornography is accessed and stored," including the ability of forensic experts to recover hidden, encrypted, or deleted files).

For similar reasons, sister circuits have also reached similar conclusions about staleness in the context of crimes involving child pornography. As the Seventh Circuit explained in *United States v. Seiver*, 692 F.3d 774, 775-76 (7th Cir. 2012):

> The concern with "staleness" versus freshness and "collecting" versus destroying reflects a misunderstanding of computer technology. (A number of cases, however, though none in our court, reflect the correct understanding. *See, e.g.*, United States v. Allen, 625 F.3d 830, 843 (5th Cir.2010); United States v. Richardson, 607 F.3d 357, 370–71 (4th Cir.2010); United States v. Lewis, 605 F.3d 395, 402 (6th Cir.2010).) When you delete a file, it goes into a "trash" folder, and when you direct the computer to "empty" the trash folder the contents of the folder, including the deleted file, disappear. But the file hasn't left the computer. The trash folder is a waste-paper basket; it has no drainage pipe to the outside. The file seems to have vanished only because the computer has removed it from the user interface and so the user can't "see" it any more. Virginia M. Kendall & T. Markus Funk, Child Exploitation and Trafficking 275–76 (2012); *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir.2011); *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir.2006) (en banc). But it's still there, and normally is recoverable by computer experts until it's overwritten because there is no longer unused space in the computer's hard drive.

Id. at 776. Citing the *Vosburgh* case from our circuit and expounding on the expansive nature of today's forensic capabilities, the *Seiver* court thus concluded that:

> "Staleness" is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file. . . . Computers and computer equipment are "not the type of evidence that rapidly dissipates or degrades. Because of overwriting, it is possible that the deleted file will no longer be recoverable from the computer's hard drive. And it is also possible that the computer will have been sold or physically destroyed. And the longer the interval between the uploading of the material sought as evidence and the search of the computer, the greater these possibilities. But rarely will they be so probable as to destroy probable cause to believe that a search of the computer will turn up the evidence sought; for probable cause is far short of certainty—it "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity," Illinois v. Gates, 462 U.S. 213, 244 n. 13, and not a probability that exceeds 50 percent ("more likely than not"), either.

Id. (internal citations omitted).

Indeed, here, the nine month gap between Google's identification of the child pornography image and Detective Dish's application for a search warrant is far from the outer limit for a staleness inquiry in a child pornography case. As noted above, the Third Circuit has upheld a similar passage of time in *Shields*, 458 F.3d at 279 n.7 (nine months). Other circuits have reached the same conclusion when assessing staleness challenges in child pornography cases. *See, e.g.,*

United States v. Schesso, 730 F.3d 1040, 1047 (9th Cir. 2013) (holding that the passage of "a mere 20 months" between a peer-to-peer download of child pornography and application for a search warrant did not render the information in the warrant stale); *United States v. Lemon*, 590 F.3d 612, 614-15 (8th Cir. 2010) (finding an 18 month gap between child pornography activity and execution of a search warrant did not render an affidavit stale); *Allen*, 625 F.3d at 843 (Fifth Circuit found information used to support search warrant was not stale even through evidence of transfer of child pornography to defendant's computer was 18 months old when the warrant issued because computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (finding three years between evidence of defendant's activities on a child pornography website and the search warrant application did not render the information stale); *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc) (finding that a four-month delay did not render information stale because "[t]hanks to the long memory of computers, any evidence of a crime was almost certainly still on his computer, even if he had tried to delete the images").

Lastly, the government notes that defendant's reliance on *Zimmerman* is misplaced. In *Zimmerman*, law enforcement obtained a search warrant for the defendant's home for both adult and child pornography; however, the affidavit contained no information suggesting that defendant possessed child pornography in his residence. 277 F.3d at 429. Thus, *Zimmerman* is in applicable to this case where the search warrant affidavit explained that a unique IP linked an electronic device in defendant Chretien's home to a Google account where the user had uploaded and saved to Google photos an image of child pornography within a day of creation of the Google account. The search warrant in this case is clearly distinguishable.

D. Suppression is an Inappropriate Remedy Because Law enforcement relied in good faith on the warrant

Even assuming for the sake of argument that no substantial basis existed for the magistrate judge's probable cause determination or that the information in the warrant was stale, the evidence obtained would nevertheless be admissible under the good faith exception to the exclusionary rule. *United States v. Abdul-Ganui*, No. 2:10CR16, 2010 WL 5279948, at *11 (W.D. Pa. Dec. 14, 2010) (Cercone, J.). When law enforcement violates the Fourth Amendment, it does not automatically warrant suppression of all future evidence. The court must determine that suppression would serve to deter future misconduct.

The Third Circuit has explained that the Exclusionary Rule does not exist to remedy a violation of the Fourth Amendment, it serves to deter government violations of the Fourth Amendment, balanced against the substantial social costs resulting from suppression; therefore, suppression of evidence should be the court's last resort. *United States v. Werdene*, 883 F.3d 204, 215 (3d Cir. 2018) (citing *Herring v. United States*, 555 U.S. 135, 140 (2009), *United States v. Krueger*, 809 F.3d 1109, 1125 (10th Cir. 2015), and *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)). "[T]he use of fruits of a past unlawful search or seizure works no new Fourth Amendment wrong." *United States v. Leon*, 468 U.S. 897, 906 (1984) (citing *United States v. Calandra*, 414 U.S. 338, 354 (1974)); *see also United States v. Katzin*, 769 F.3d 163, 177 & 182 (3d Cir. 2014) (citing *Leon*, 468 U.S. at 922 n.23 and stating that when considering whether the good faith exception applies, courts should "consider the totality of the circumstances to answer the 'objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal.'")

Suppression of the evidence from defendant's residence would not serve to deter police misconduct, particularly when balanced against the significant social cost suppression of this

evidence would cause. *See Leon*, 468 U.S. at 909. Suppression would be an inappropriate remedy because law enforcement acted with a good faith belief in the lawfulness of their conduct when they obtained a search warrant for defendant's residence, and that belief was "objectively reasonable." *Leon*, 468 U.S. 897 (1984) (suppression not warranted if search warrant later found to lack probable cause was executed in good faith). Suppression of the evidence law enforcement obtained through valid legal process would not serve to deter police misconduct. Detective Dish outlined facts, given his experience and training, which established probable cause to search the defendant's residence; presented this evidence in an affidavit to a neutral judge; and searched the location pursuant to a validly issued search warrant. These steps all respect defendant's Fourth Amendment rights, and suppression is not warranted.

E. The "Fruit of the Poisonous Tree" Doctrine is Inapplicable Here

Defendant submits that the search warrant for defendant's residence was invalid and therefore any subsequent warrants, as well as any subsequent incriminating statements made by defendant constitute "fruit of the tree" and should be suppressed.

The fruit of the poisonous tree doctrine, discussed in *Wong Sun v. United States*, relies on the argument that but for the illegal police seizure, the government would never have had access to the evidence, even if obtained through appropriate police action. *Wong Sun v. United States*, 371 U.S. 471, 487-488 (1963).

However, as explained above, law enforcement entered and searched defendant's residence pursuant to a lawful search warrant. The facts included in the affidavit were relevant, not stale, and established probable cause that violations of Pennsylvania's sexual abuse of children laws would be found in defendant's residence. Quite simply, the warrant was valid and any subsequent search warrants or statements obtained from defendant are not fruit of the poisonous tree.

III. CONCLUSION

For all of the foregoing reasons, defendant's Motion to Suppress Evidence, Doc. No. 29, should be denied.

Respectfully submitted,

SCOTT W. BRADY
United States Attorney

s/Heidi M. Grogan
HEIDI M. GROGAN
Assistant U.S. Attorney
PA ID No. 203184